INFONET

SafeNet™

Pure VPN Solutions from IRE

VPN Client

クイックスタートガイド

古河電工

www.furukawa.co.jp

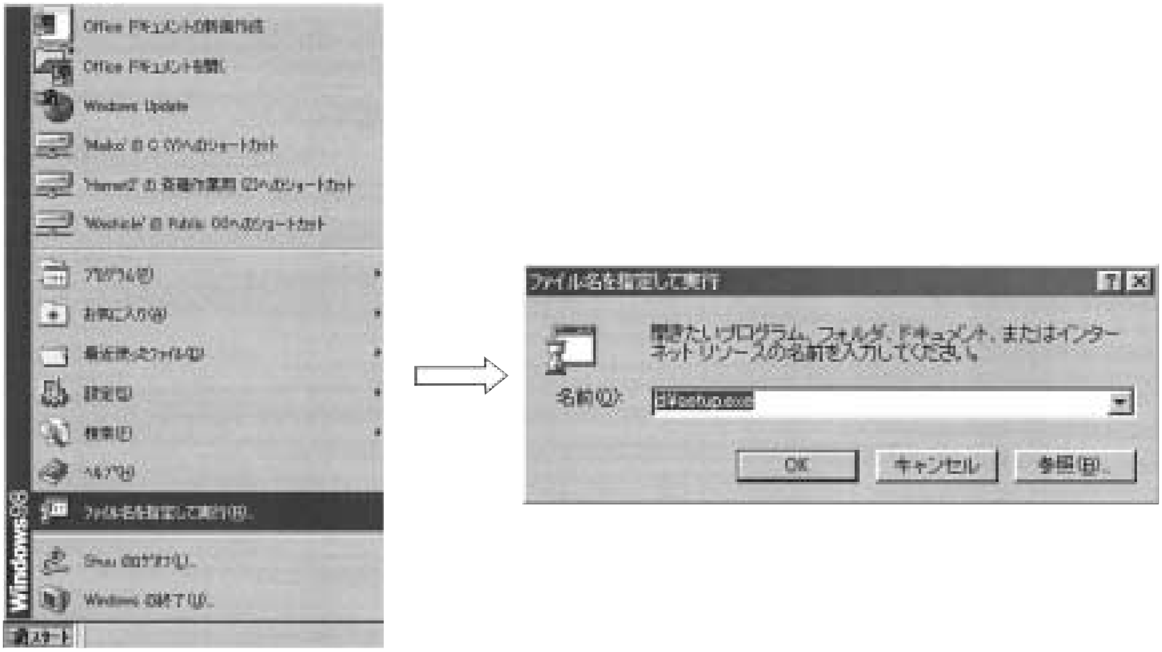
（注　意）

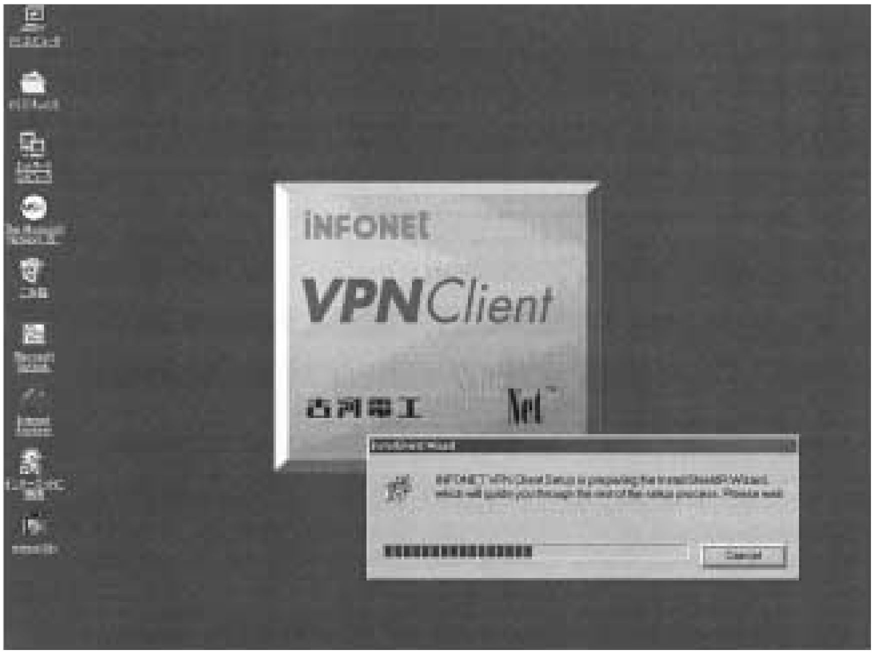
●ここに示した手順は、設定の一例です。各手順の詳細については、各基本ソフトウェアのマニュアル及びヘルプ、モデム及びターミナルアダプタの取扱説明書をご参照ください。
●モデム及びターミナルアダプタが正しくパソコンに接続されているかどうか、あらかじめお確かめ下さい。接続方法については、モデム等の取扱説明書をご参照ください。

（目　次）

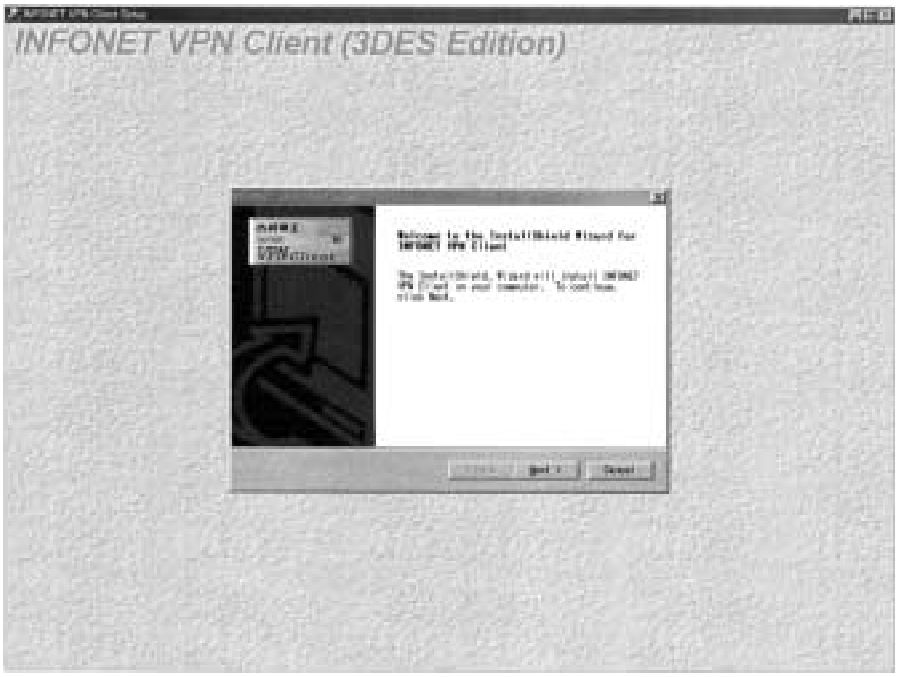
ステップ１
VPN クライアントソフトフェアのインストール

1. スタートメニューから、「ファイル名を指定して実行」を選択した後、「d：\setup.exe」（CD-ROM が D：の場合）と入力し「OK」をクリックします。インストーラが起動します。

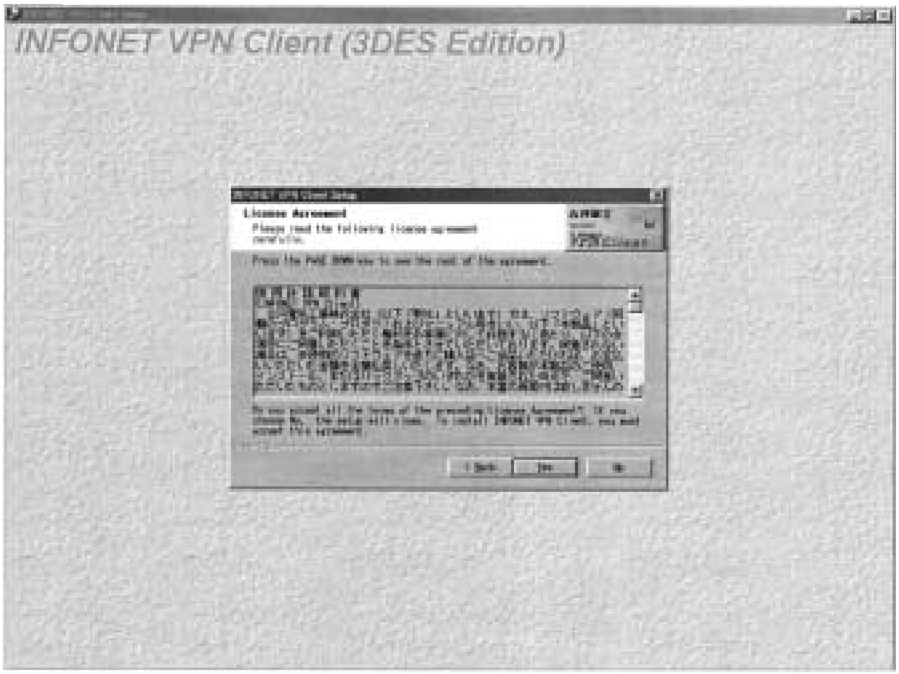




2. Next ＞ をクリックします。

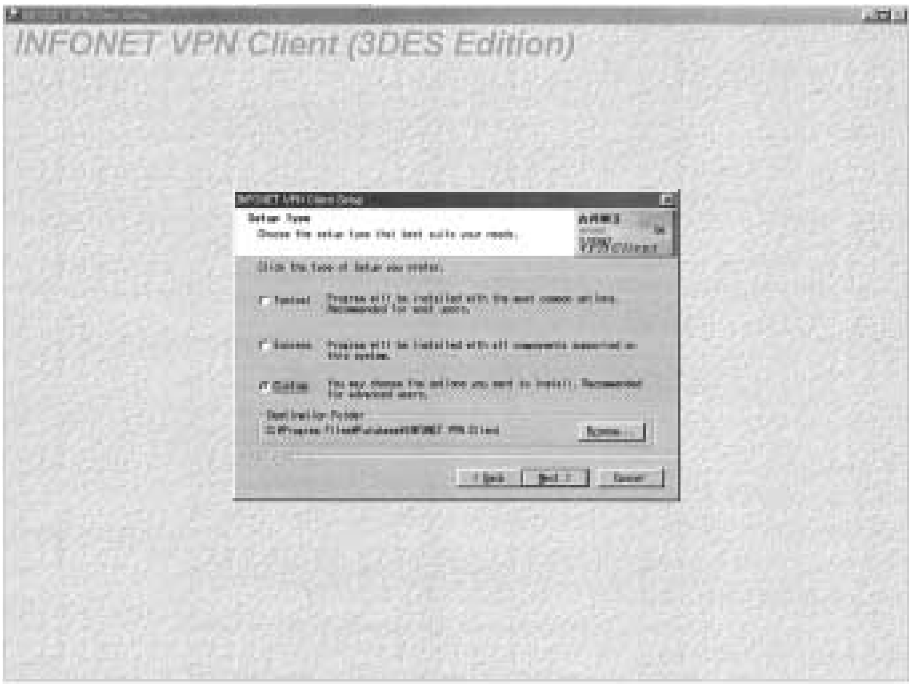


3. 使用許諾契約書をよく読み、同意する場合は Yes ＞ をクリックします。

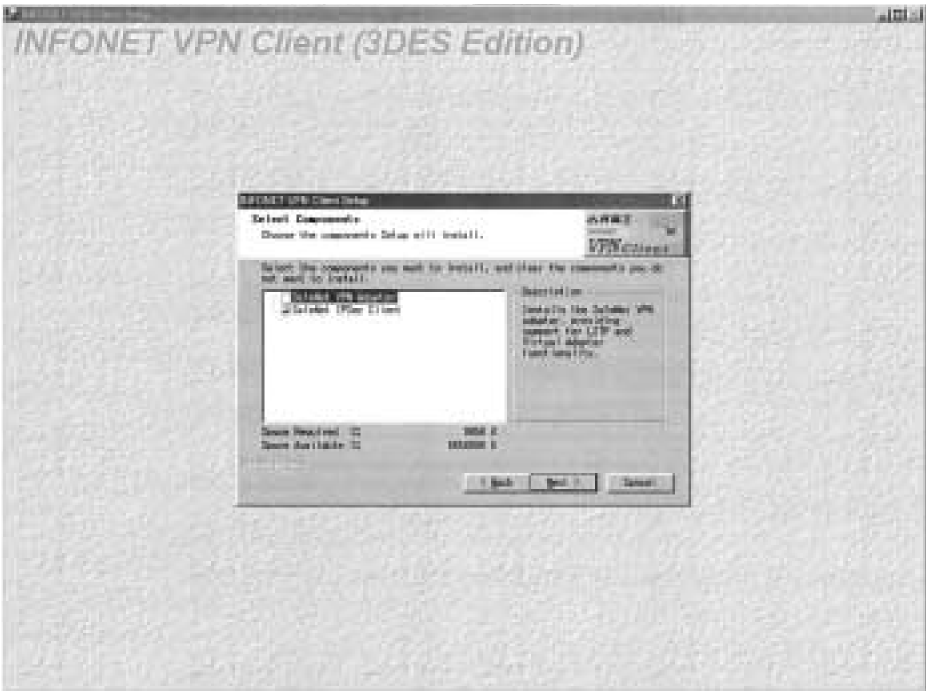


ＶＰＮ クライアントソフトフェアのインストール

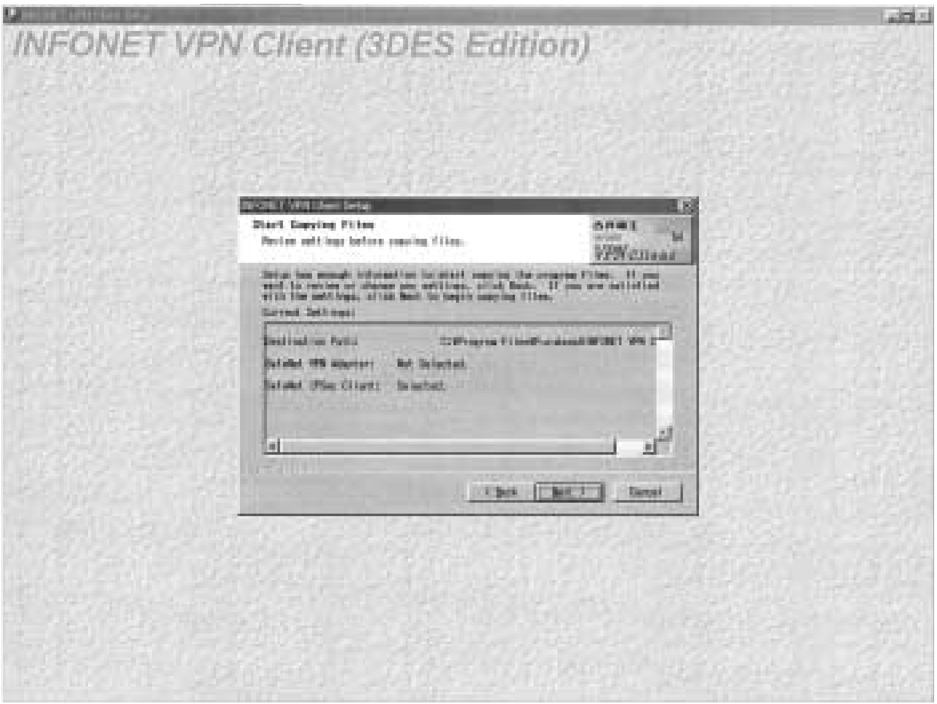
4. インストール方法は " Custom " を選択、およびインストールディレクトリ（通常はデフォルトのままで構いません）を選択し、 Next ＞ をクリックします。



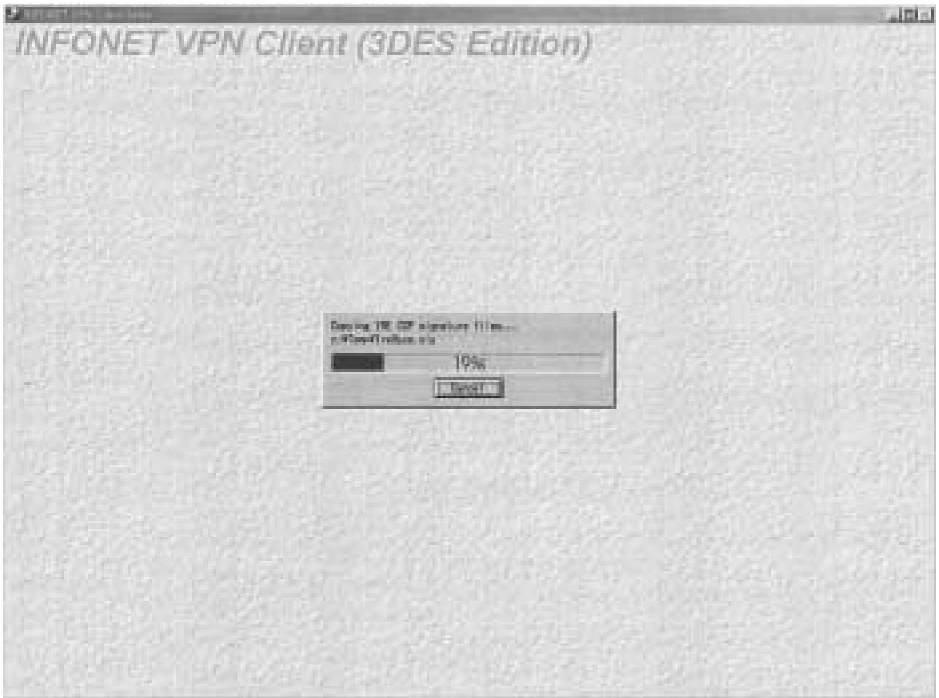
5. Safenet VPN Adapter のチェックを外し、 Next ＞ をクリックします。



6．設定内容を確認し、Next ＞ をクリックします。

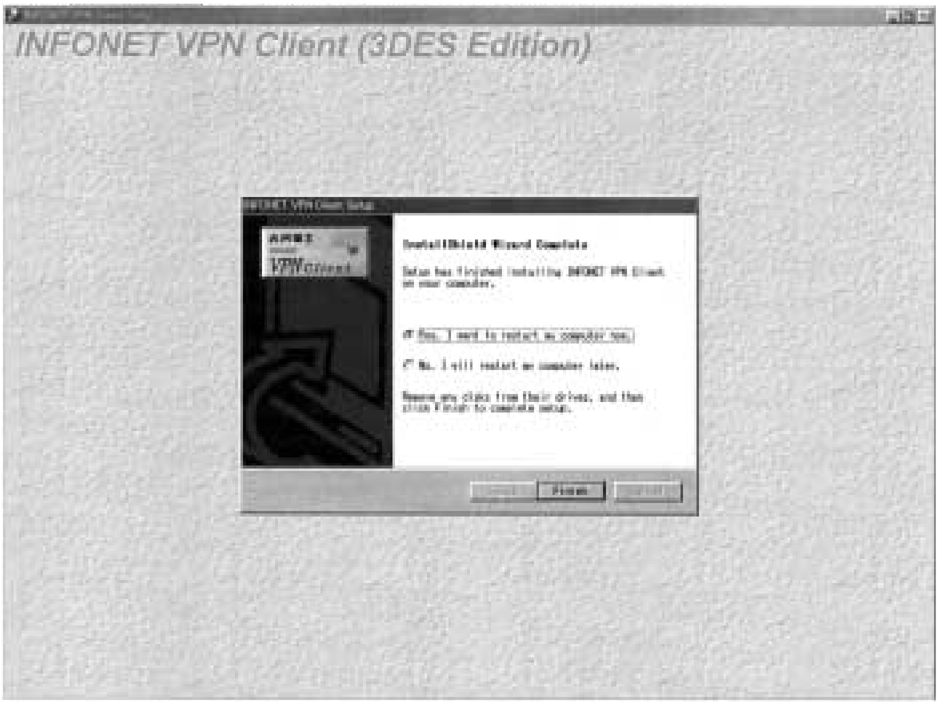


7．必要なファイルがインストールされます。



ステップ１
VPN クライアントソフトフェアのインストール

8. インストールが完了すると、再起動が必要になります。他のアプリケーションを全て終了させ、 Finish ＞ をクリックすると、再起動が始まります。



ステップ２
ダイヤルアップの準備

【ご注意】

このステップ２では、一般的なダイヤルアップの設定方法について説明しています。
設定は、モデムの機種や設定状況、利用されるプロバイダの最寄のアクセスポイント電話番号によって設定内容が異なりますのでご注意下さい。
詳しくは、モデム購入先もしくは利用されるプロバイダにお問い合わせ下さい。

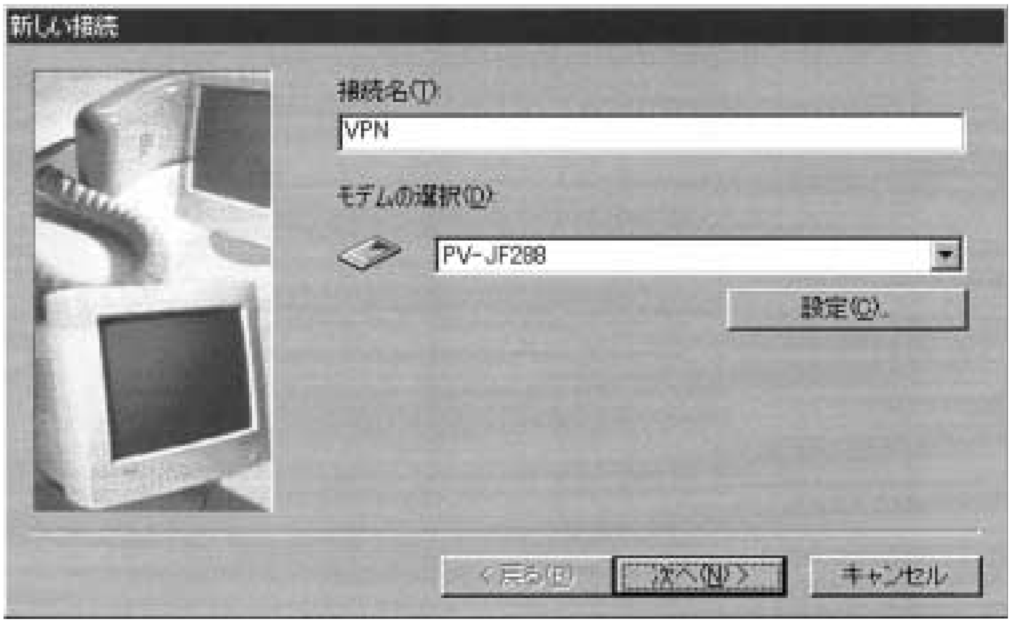
1. 画面左上部にある「マイ　コンピュータ」をダブルクリックして、「ダイヤルアップ　ネットワーク」をダブルクリックします。



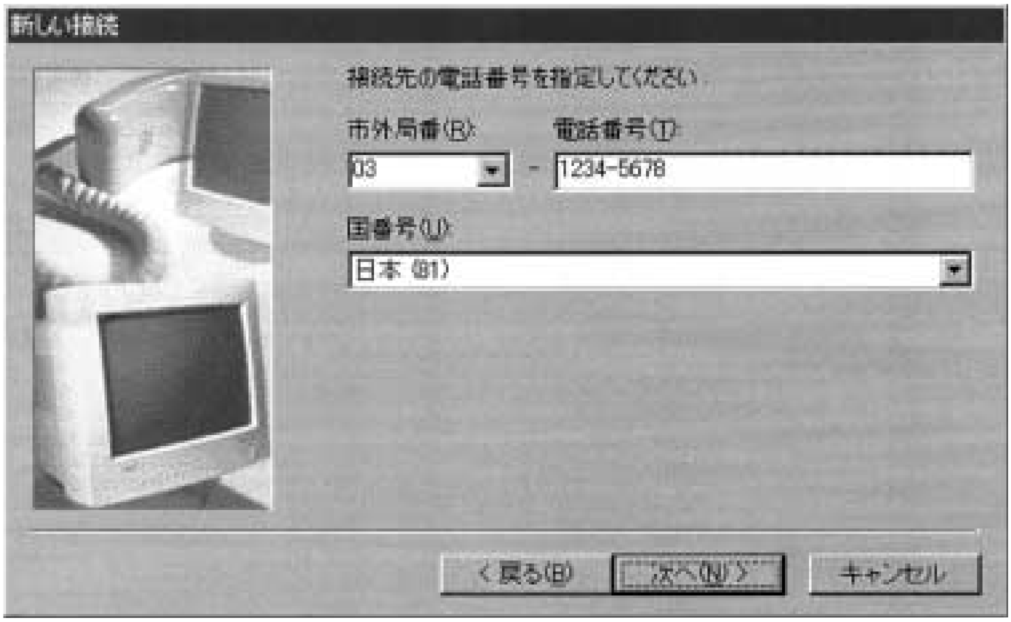
2. 「新しい接続」をダブルクリックします。



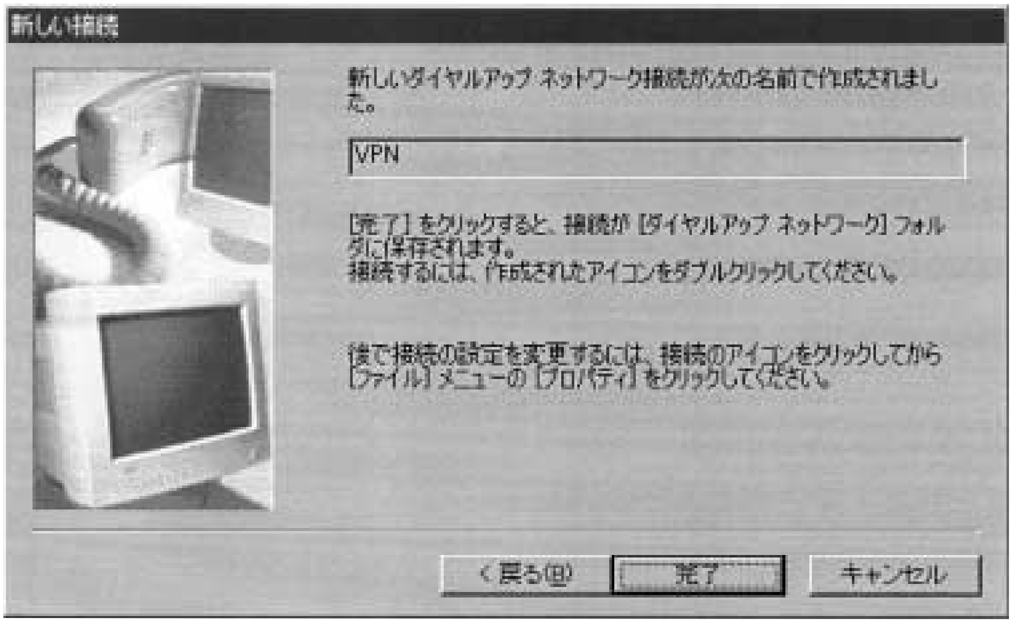
3. 接続名とモデムの設定をします。接続名を入力し、ご利用になるモデムを選択します。 次へ をクリックします。



4. 接続先の設定をします。ご利用になる回線種別に合った最寄りのアクセスポイントの電話番号を、入力します。国番号は、「日本（81)」を選択します。 次へ をクリックします。



5. 完了 をクリックします。

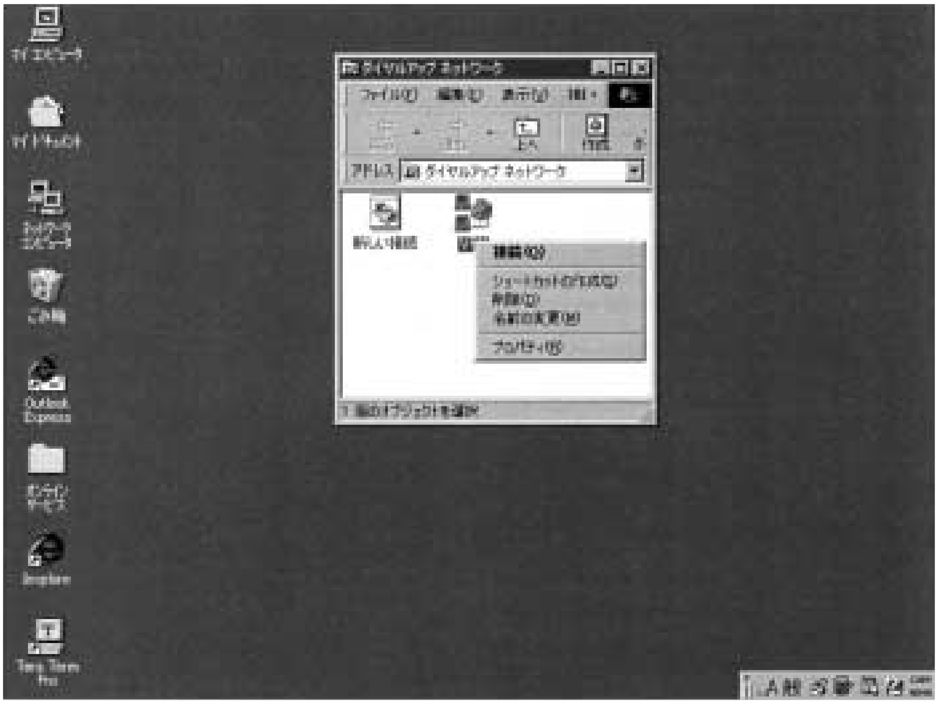


ステップ３
接続ファイルのプロパティ設定

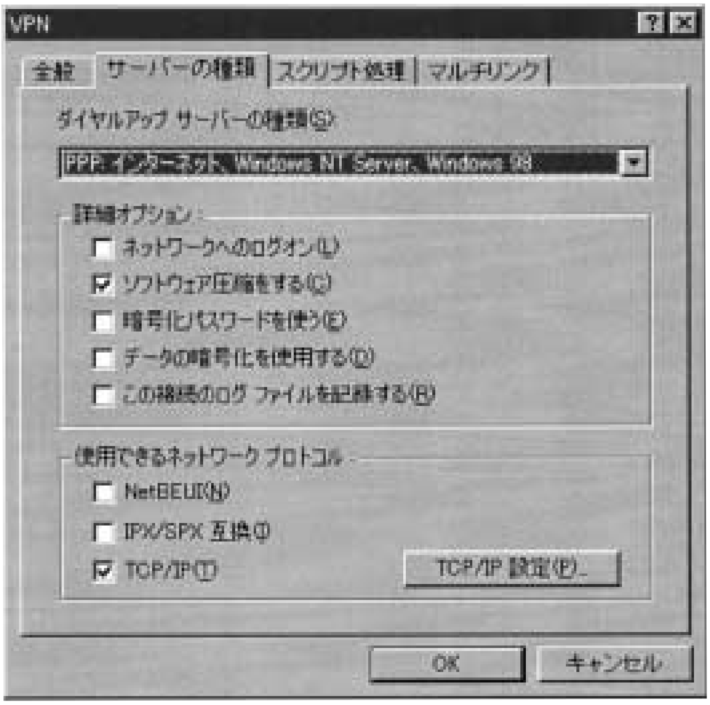
１．「ダイヤルアップ　ネットワーク」を開きます。



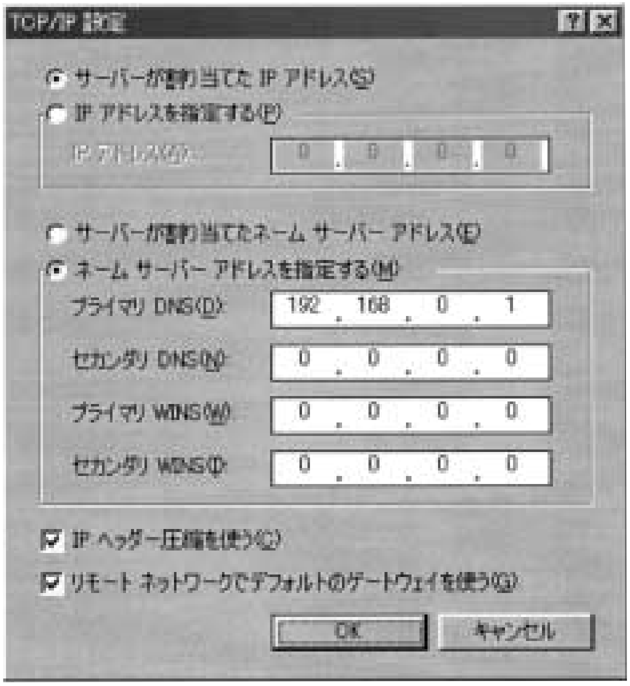
２．作成した「VPN」を選び、右クリックして「プロパティ」を開きます。



3． **サーバーの種類** **タブをクリックします。この設定は接続するプロバイダにより異なります。**



4． **TCP／IP** **設定をクリックします。以下のように設定します。**
（※この画面は基本ソフトウェアのバージョンによって異なる場合があります。）



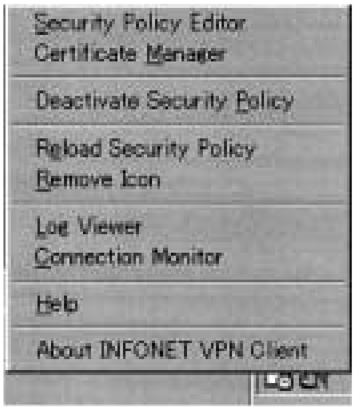
5． **OK** **を２回クリックして画面を閉じます。**

ステップ４
デジタル証明書の取得

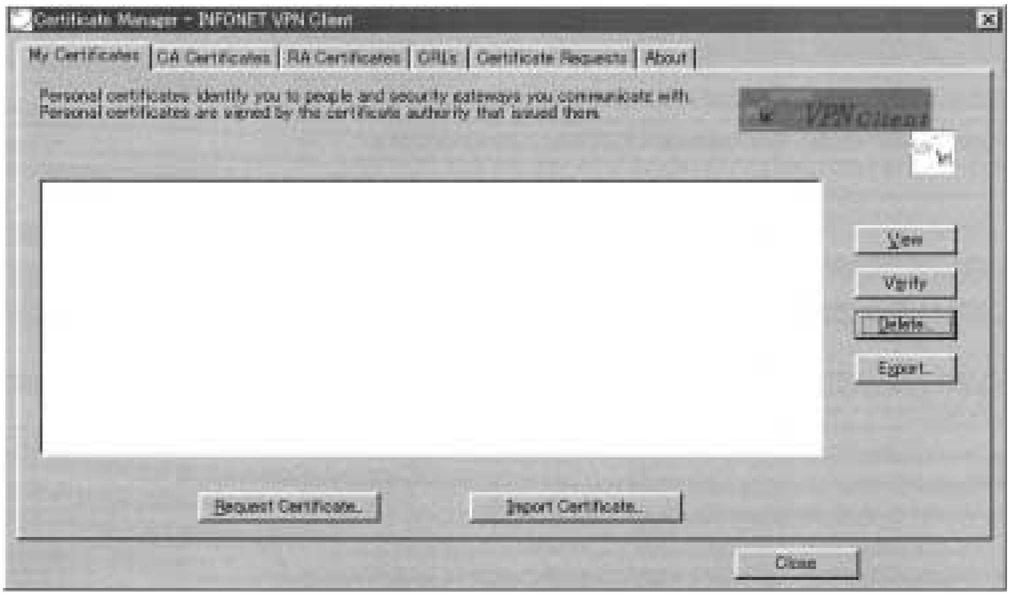
X.509機能を使用する場合には、CA からのデジタル証明書の発行が必要となります。pre-shared キーを使用する場合には、ステップ５に進んでください。
X.509機能は、証明書を CA センターに依頼し、改ざん・なりすましを防ぐ技術であり、INFONET-VP100、MUCHO-EV／PK で対応している機能です。

1．タスクバーの  **のアイコンを右クリックし、メニューから「Certificate Manager」を選択します。**

Certifacate Manager ウィンドウが表示されます。

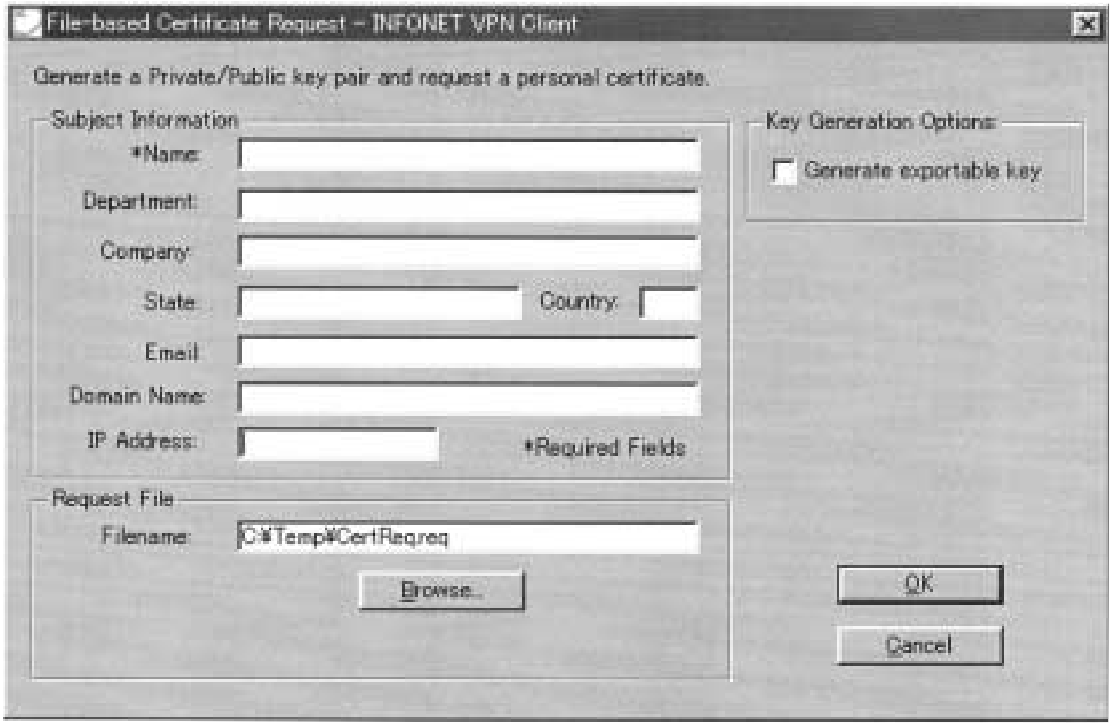


2．「証明書請求ファイルを作成するために、「My Certificates」タブをクリックし「Request Certificate」ボタンをクリックします。



・オンライン（CEP）登録用に設定された CA 証明書が存在しない場合は、ファイルによる請求を行うように指示するプロンプトが表示されます。Yes をクリックして、File-based Certificate Request ダイアログ・ボックスを開いてください。
・オンライン（CEP）登録用に設定された CA 証明書が存在する場合は、On-line Certificate Request ダイアログ・ボックスが表示されます。Enrollment method から File を選択してください。

3. 個人情報を入力します。



●Subject Information の下に個人情報を入力します。ダイアログ・ボックス内のフィールド間を移動するには、 Tab キーを押します。

注記： Enter キーを押すと、一部の情報が入力されていない状態で請求データが作成されてしまいます。

●CA に送信する証明書請求ファイルのドライブ、ディレクトリ、ファイル名を Request File に入力します。デフォルトは C:¥Temp¥CertReq. req です。

●OK をクリックします。パブリック・キーとプライベート・キーのペアが Certificate Manager によって生成された後、証明書請求ファイルが作成されたというメッセージが表示されます。OK をもう一度クリックしてください。

●任意指定：請求データの内容を表示するには、Certificate Requests タブをクリックし、目的の請求データを選択して View をクリックします。このウィンドウを閉じるには、ウィンドウの内部をクリックします。

4．CA から証明書を発行してもらいます。

デジタル証明書を取得するには、認証局（CA）に登録する必要があります。主な登録方法は次の２通りです。

- CEP（Certificate Enrollment Protocol）を使用するオンライン登録－オンライン登録をサポートする CA を選択した場合は、その CA から CA 証明書を取得してからでないと、パーソナル証明書をオンライン請求することができません。オンライン請求を行うときは、証明書サーバの DNS 名または IP アドレスを事前に知っておく必要があります。
- テキスト・エディタからのカット＆ペーストを必要とするマニュアル登録－CA はさまざまな方法でマニュアル登録を処理しますが、最初に必ず上述した証明書請求ファイルを作成する必要があります。パブリック・キー／プライベート・キーのペアは、Certificate Manager によって自動的に作成されます。パブリック・キーは証明書請求ファイルとともに送信され、プライベート・キーはハードディスク上に残ります。

  CA によっては、証明書請求ファイルをテキスト・ファイルで開き、CA の Web サイト上のフィールドに情報をコピー＆ペーストする場合や、例えば電子メールなどで受け取ったパーソナル証明書をテキスト・エディタにコピー＆ペーストしてファイルを作成し、そのファイルを Certificate Manager にインポートする場合などもあります。

〔参考〕

デジタル証明書は、VeriSign、Netscape、Entrust などの認証局（CA：certificate authority）に請求する必要があります。デジタル証明書を取得してから、セキュリティ・ポリシーの定義に取り掛かってください。

個々のＣＡによって処理手続きが異なるため、デジタル証明書の請求や受け取りの詳しい手順については、選択したＣＡに直接問い合わせてください。Certificate Manager は、CA 証明書とパーソナル証明書の請求、取得、インポートに必要なほとんどの手続きに対応しています。

無料のトライアル証明書：　ユーザの便宜を図るために、IRE と VeriSign はトライアル証明書を無料で提供するサービスを用意しています。このサービスを利用すると、INFONET VPN Client 環境でデジタル証明書のテストを行うことができます。無料の CA 証明書（トラスト・チェーンを作成できるルート証明書）または最大20個の無料パーソナル証明書を入手するには、次の Go Secure Web サイトにアクセスしてください。

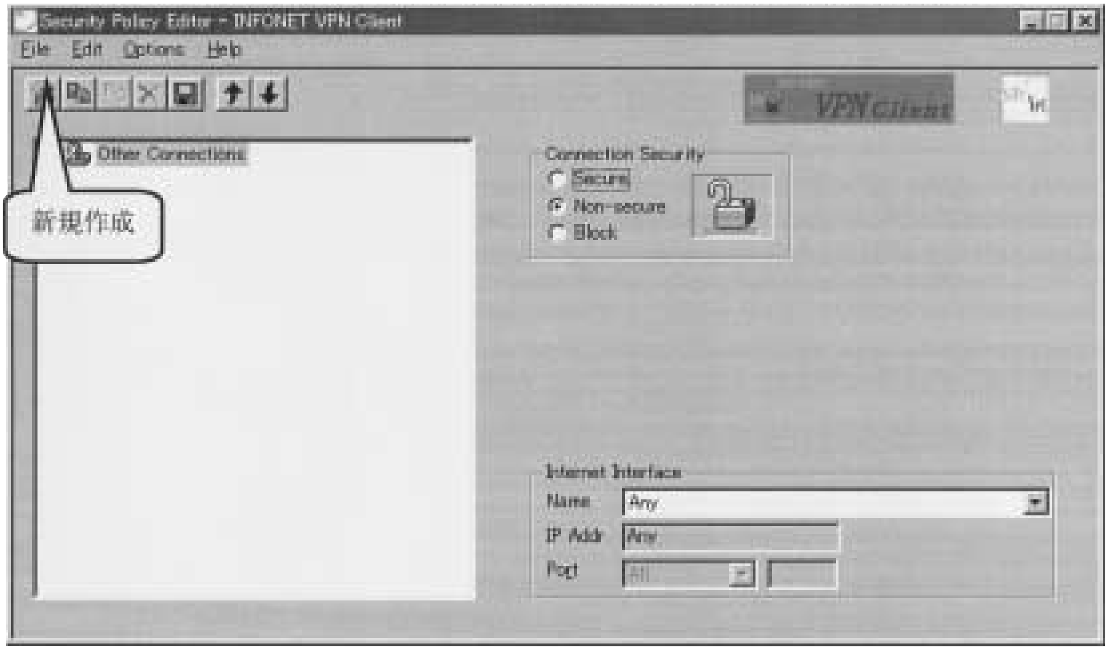
http : //www. ire. com/security/Go_Secure. htm

注意：これらの無料証明書はテスト環境のみで使用することを前提としています。企業の機密通信を保護するのに必要な本番環境のセキュリティは保証されませんので、十分にご注意ください。

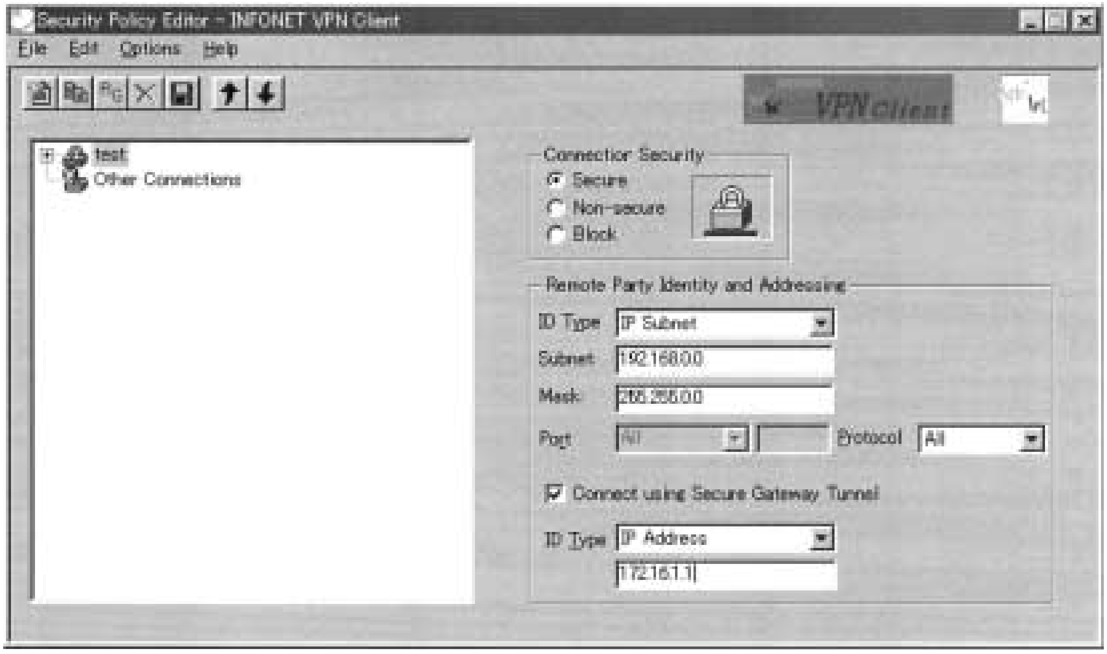
ステップ５

VPN クライアントのプロパティ設定（pre-shared キー編）

1．タスクバーの  のアイコンをダブルクリックします。「Security Policy Editor」というウィンドウが開きます。ウィンドウの上部分に並んだツールボタンの一番左をクリックします。



2. 緑色の新しいコネクションが作成されますので、名前を「test」と入力します。右側の設定は以下の図のように設定します。



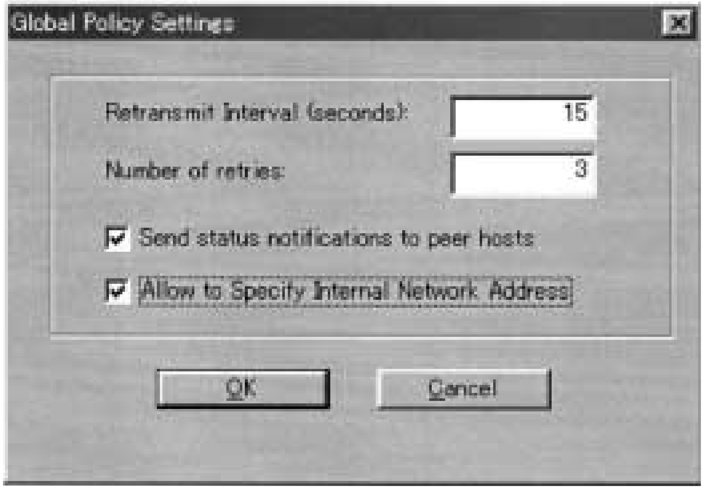
Connection Security
　◎Secure
　○Non-Secure
　○Block

Remote Party Identity and Addressing（暗号化するパケットの指定）
　ID Type ：IP Subnet
　Subnet ：192.168.0.0
　Mask ：255.255.0.0
　Protocol ：All
この例では、192.168.0.0～192.168.255.255宛の IP パケットが暗号化の対象となります。

Connect using Secure Gateway Tunnel —> チェックあり（IPsecトンネルの相手のアドレス）
　ID Type ：IP Address
　　　　　172.16.1.1
この例では、IPsec トンネルの相手のアドレスが172.16.1.1となります。

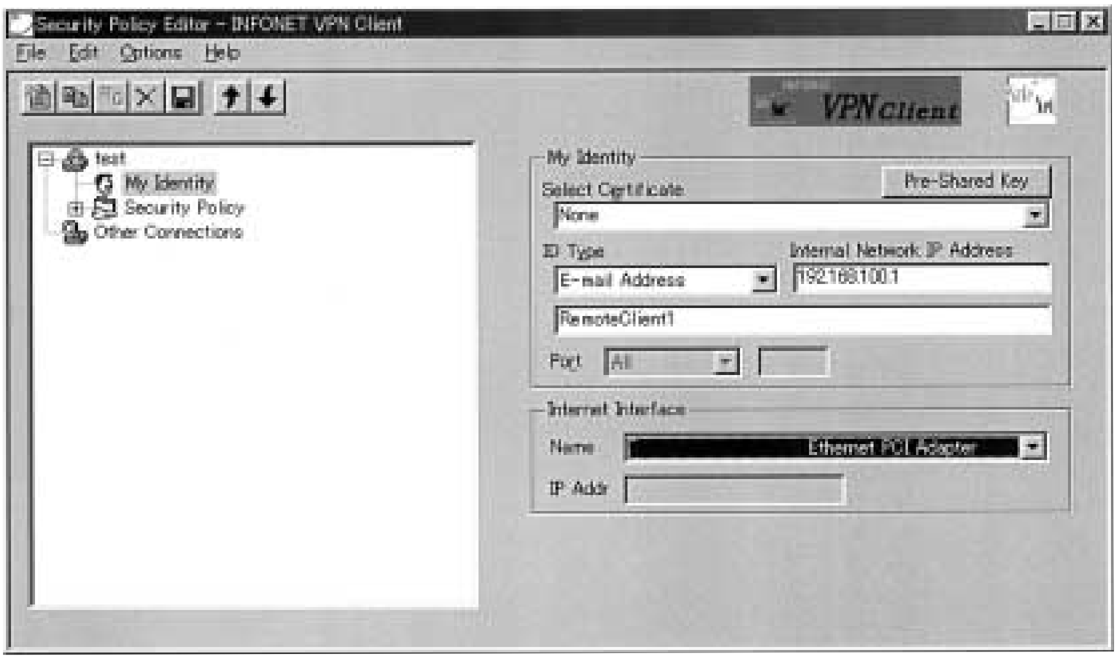
ステップ５
VPN クライアントのプロパティ設定（pre-shared キー編）

3. ウィンドウのメニューから［Options］ー＞［Global Policy Settings］を選択すると、以下のウィンドウが開きますので、以下の図のように設定します。



Retransmit Interval（seconds）：15
Number of retries　　　　　　　：３
■Send status notifications to peer hosts ー＞ チェックあり
■Allow to Specify Internal Network Address ー＞ チェックあり

4. 左側のアイコン「test」の「+」をクリックします。メニューが開きますので左側のアイコン「My Identity」をクリックして選択します。ここでは、自身の情報を設定します。



My Identity

Select Certificate：None
ID Type　　　　　：E-mail Address
　　　　　　　　　Remote Clientl

※ : Main Mode で使用する場合は、ID Type に IP アドレスを選択してください。

Internal Network IP Address：192.168.100.1

※：Internal Network IP Address は、アクセスするサーバと TCP／IP の通信が可能な IP アドレスを指定してください。指定する IP アドレスはネットワーク管理者にご相談ください。

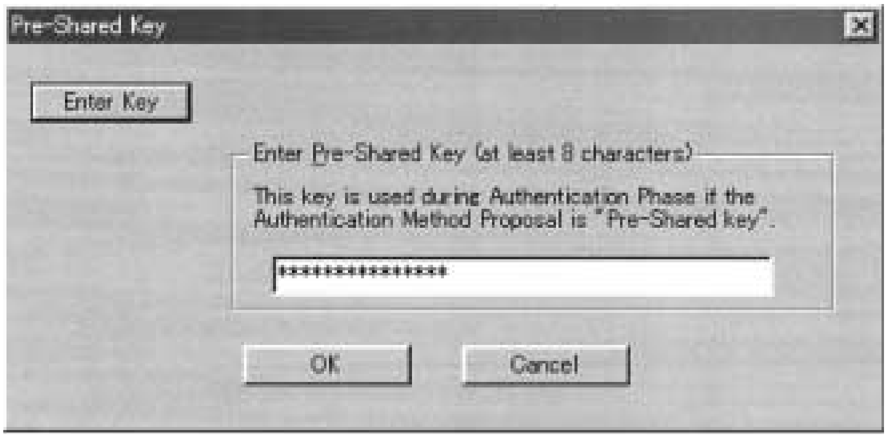
Internal Network IP Address は、リモート側の LAN のネットワークの中から割り当てることで、サブネットの不要な切り出しを回避し、アドレス利用効率を上げることが可能になります。
そのため、センター側（INFONET-VP100など）は、Proxy ARP を動かす必要があります。

Internet Interface

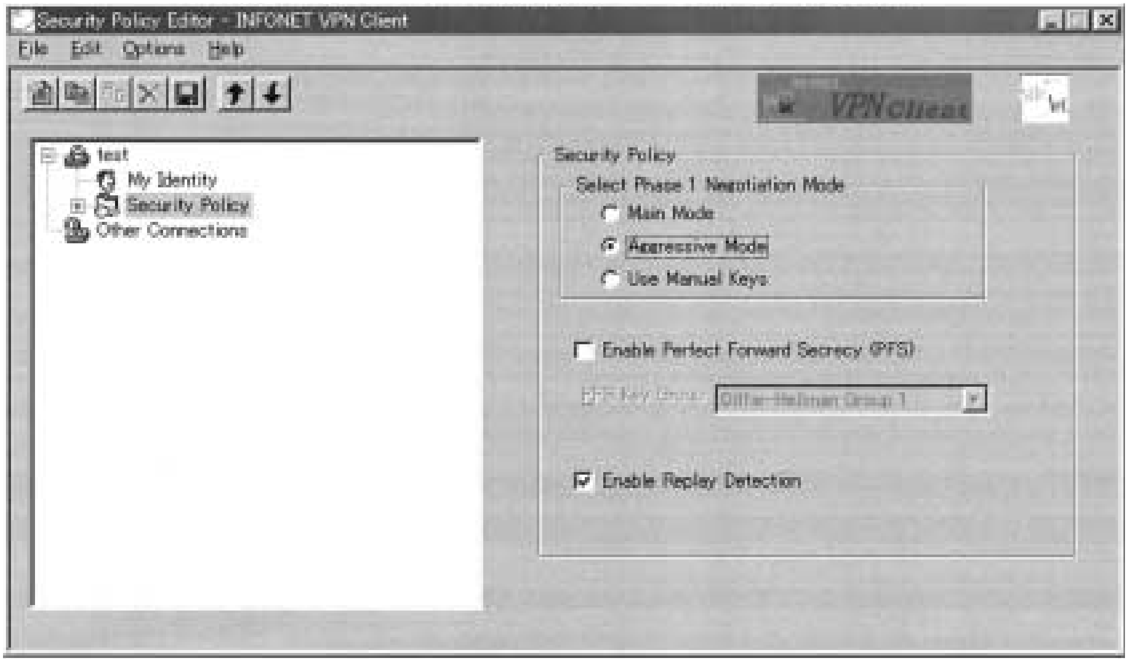
VPN 通信を行うインタフェースを選択してください。

VPN クライアントのプロパティ設定（pre-shared キー編）

5.「My　Identity」ウィンドウ内の「Pre-Shared　Key」をクリックすると新しいウィンドウが開きます。
ウィンドウ内の「Enter Key」ボタンをクリックすると、「Enter Pre-Shared Key (at least 8 characters)」欄に入力できるようになります。
管理者より発行された　Pre-Shared Key　を入力し、 OK をクリックします。



6. 左側のアイコン「Security Policy」をクリックして選択し、以下の図のように設定します。



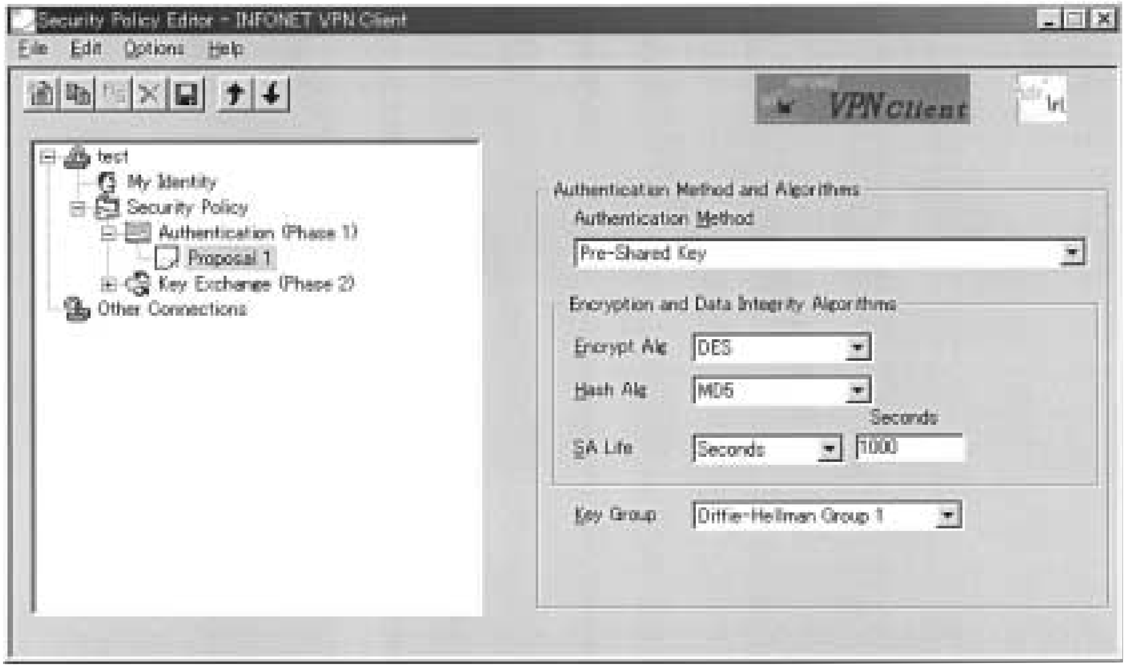
Select Phase 1 Negotiation Mode
　○Main Mode
　◎Aggressive Mode
　○Use Manual Keys

Enable Perfect Forward Secrecy（PFS）　－＞ チェックなし

Enable Replay Detection －＞ チェックあり

VPN クライアントのプロパティ設定（pre-shared キー編）

7．左側アイコン「Security Policy」の「＋」をクリックしてメニューを開きます。
「Authentication（Phase １）」の「＋」をクリックしてメニューを開きます。
「Proposal １」をクリックして選択し、以下のように設定します。



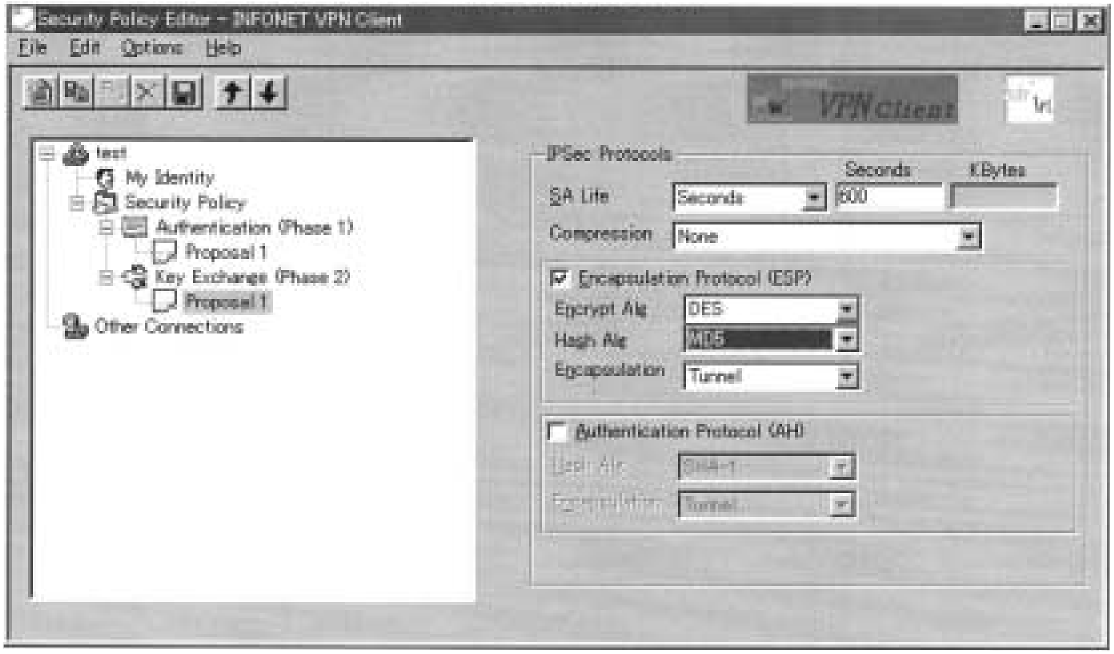
Authentication Method
　Pre－Shared key

Encryption and Data Integrity Algorithms
　Encrypt Alg：DES※
　Hash Alg　：MD５※
　SA Life　　：1000 seconds※

Key Group
　Diffie-Hellman Group１※

※：この設定は、IPsec トンネルを確立する相手と同じでなくてはいけません。

8. 左側のアイコン「Key Exchange（Phase２）」の「+」をクリックしてメニューを開きます。
「Proposal１」をクリックして選択し、以下の図のように設定します。



IPSec Protocols
SA Life　　　：600 seconds※

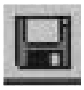
Encapsulation Protocol（ESP）—＞ チェックあり
Encrypt Alg　：DES※
Hash Alg　　：MD５※
Encapsulation：Tunnel

Authentication Protocol（AH）—＞ チェックなし

※：この設定は、IPsec トンネルを確立する相手と同じでなくてはいけません。

9. VPN として通過させたいネットワークあるいは IP アドレス毎に一つのコネクションを作成します。

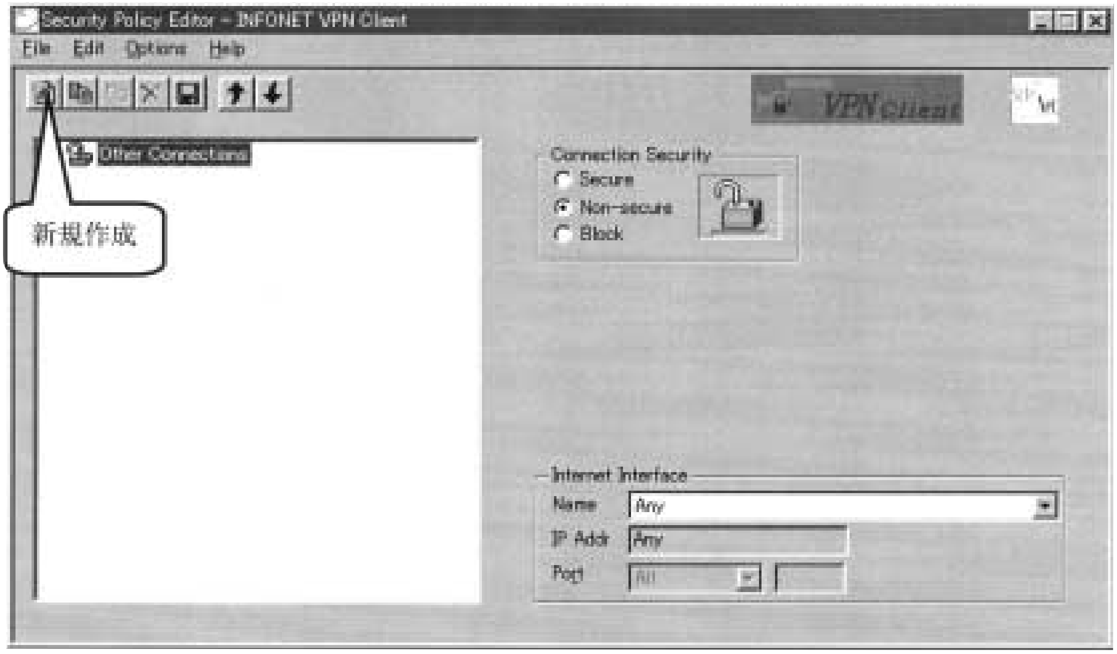
10. 新しいコネクション毎について、「test」と同様に４～８の設定を行います。設定項目および入力値については、「test」と同じです。

11. すべての設定が完了したら、ツールバーの  をクリックし、設定を保存します。

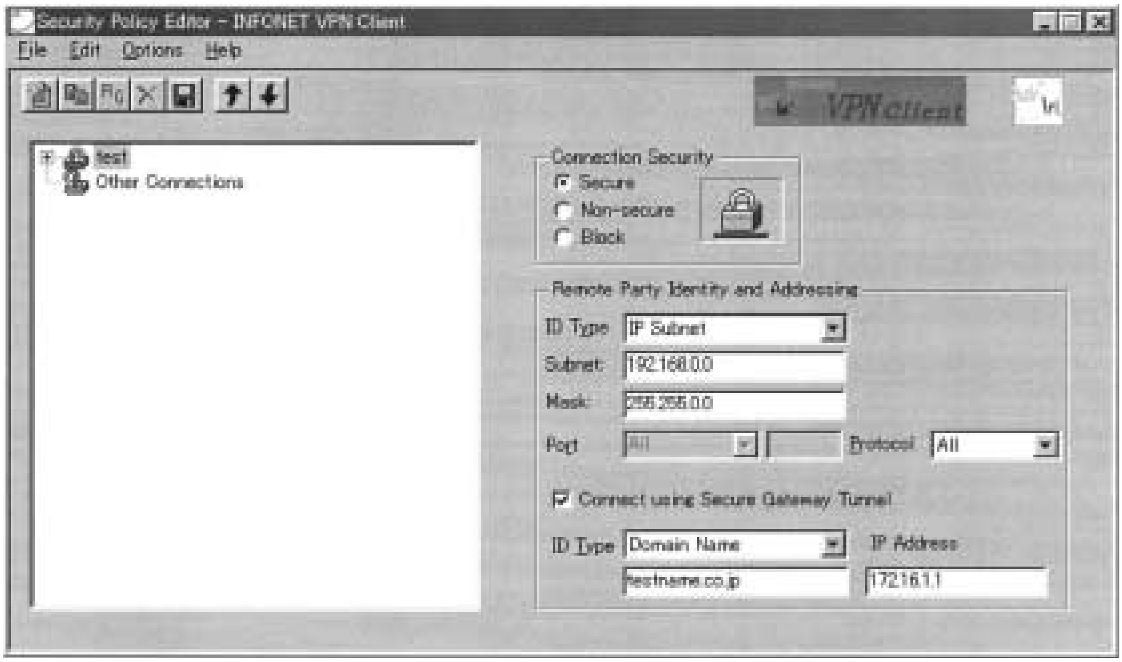
ステップ６
ＶＰＮ クライアントのプロパティ設定（Ｘ.509編）

1. タスクバーの  のアイコンをダブルクリックします。「Security Policy Editor」という

ウィンドウが開きます。ウィンドウの上部分に並んだツールボタンの一番左をクリックします。



2. 緑色の新しいコネクションが作成されますので、名前を「test」と入力します。右側の設定は以下の図のように設定します。



Connection Security
◎Secure
◯Non-Secure
◯Block

Remote Party Identity and Addressing（暗号化するパケットの指定）
ID Type　：IP Subnet
Subnet　：192.168.0.0
Mask　：255.255.0.0
Protocol　：All
この例では、192.168.0.0～192.168.255.255宛の IP パケットが暗号化の対象となります。

Connect using Secure Gateway Tunnel　–>　チェックあり（IPsecトンネルの相手のアドレス）
ID Type　：Domain Name
相手のドメイン名を入力※
IPAddress：172.16.1.1

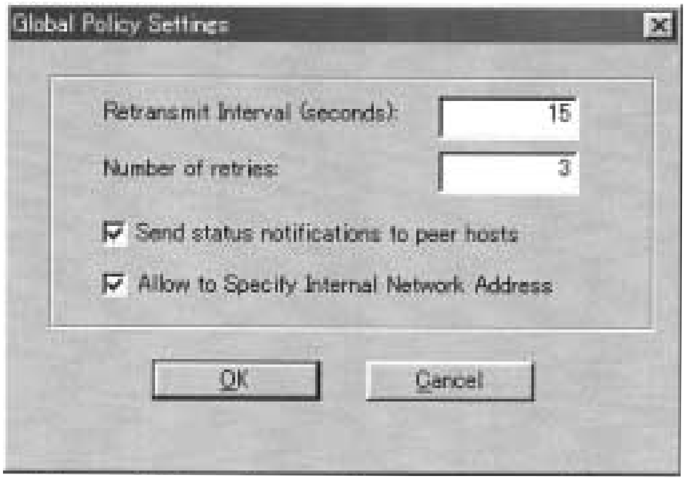
この例では、IPsec トンネルの相手のドメイン名が “ testname.co.jp ”、のアドレスが172.16.1.1となります。

※：相手の設定内容と同じでなくてはいけません。

ステップ６

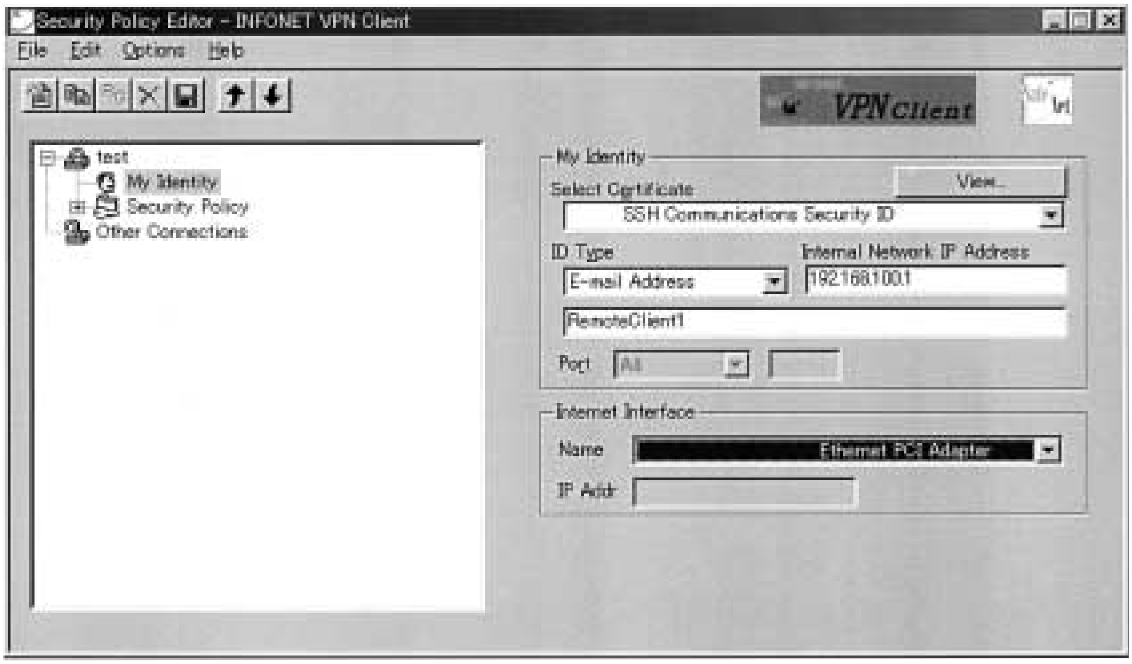
ＶＰＮ クライアントのプロパティ設定（Ｘ.509編）

３. ウィンドウのメニューから［Options］－＞［Global Policy Settings］を選択すると、以下のウィンドウが開きますので、以下の図のように設定します。



Retransmit Interval（seconds）：15
Number of retries　　　　　　　：３
■Send status notifications to peer hosts －＞ チェックあり
■Allow to Specify Internal Network Address －＞ チェックあり

4. 左側のアイコン「test」の「+」をクリックします。メニューが開きますので左側のアイコン「My Identity」をクリックして選択します。ここでは、自身の情報を設定します。



My Identity

Select Certificate　：取得したデジタル証明書を選択します。
ID Type　：Email-address
Remote Clientl
Internal Network IP Address：192.168.100.1

※：Internal Network IP Address は、アクセスするサーバと TCP／IP の通信が可能な IP アドレスを指定してください。指定する IP アドレスはネットワーク管理者にご相談ください。

Internal Network IP Address は、リモート側の LAN のネットワークの中から割り当てることで、サブネットの不要な切り出しを回避し、アドレス利用効率を上げることが可能になります。
そのため、センター側（INFONET-VP100など）は、Proxy ARP を動かす必要があります。

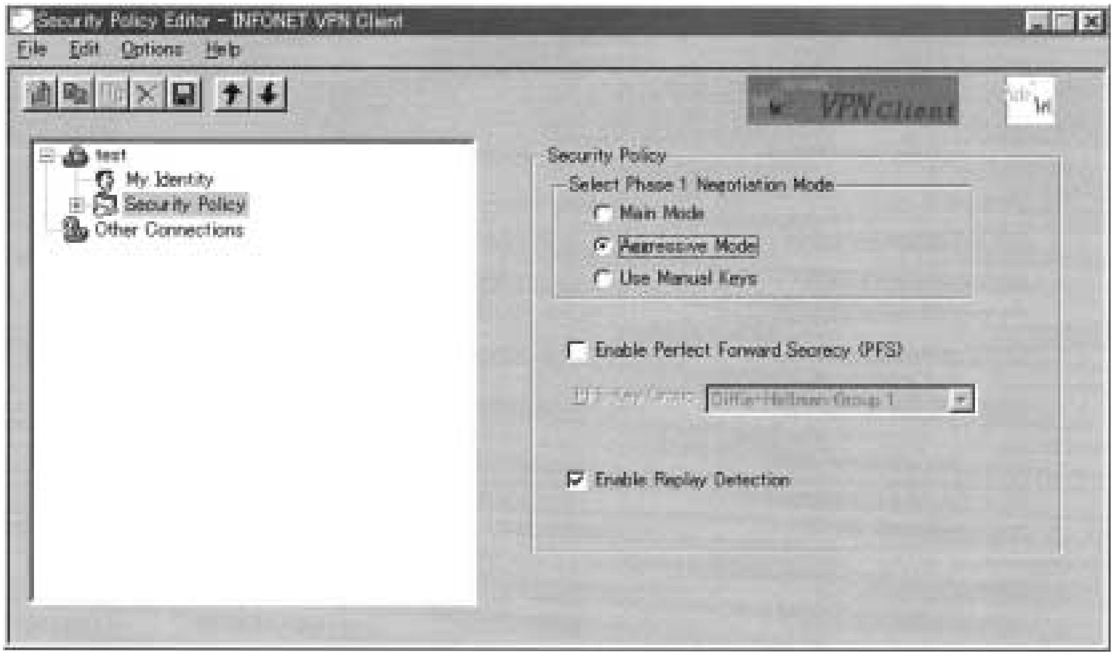
Internet Interface

VPN 通信を行なうインタフェースを選択してください。

ステップ６

ＶＰＮ クライアントのプロパティ設定（Ｘ .509編）

5．左側のアイコン「Security Policy」をクリックして選択し、以下の図のように設定します。



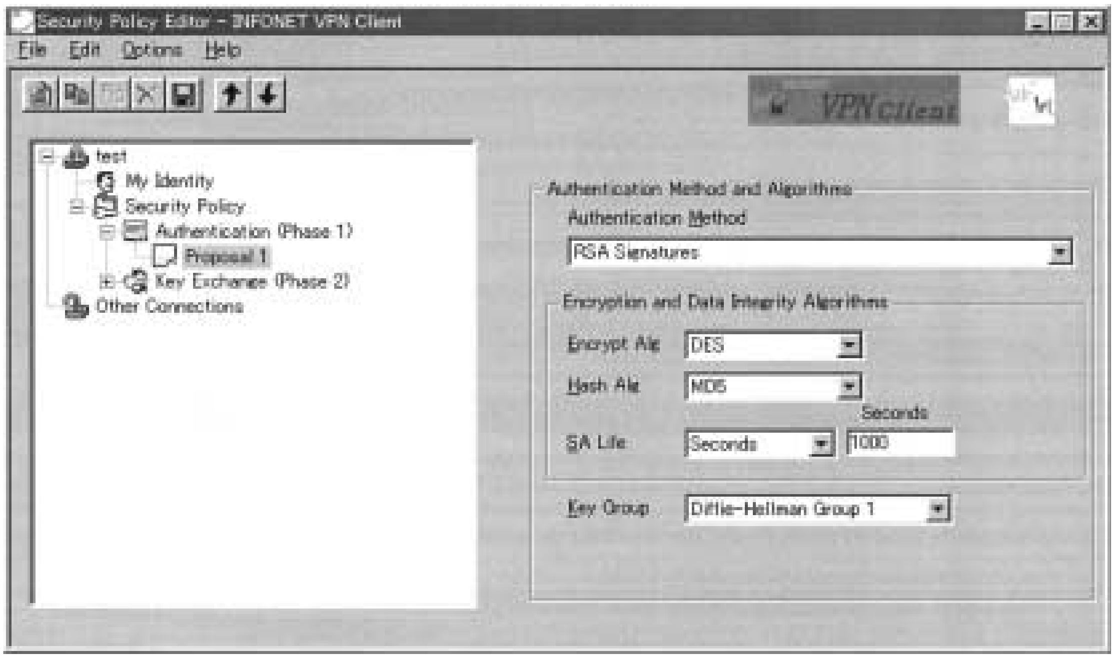
Select Phase１Negotiation Mode

〇Main Mode
◎Aggressive Mode
〇Use Manual Keys

Enable Perfect Forward Secrecy（PFS）－＞ チェックなし

Enable Replay Detection －＞ チェックあり

6. 左側アイコン「Security Policy」の「+」をクリックしてメニューを開きます。
「Authentication（Phase１）」の「+」をクリックしてメニューを開きます。
「Proposal１」をクリックして選択し、以下のように設定します。



Authentication Method

RSA Signatures

Encryption and Data Integrity Algorithms

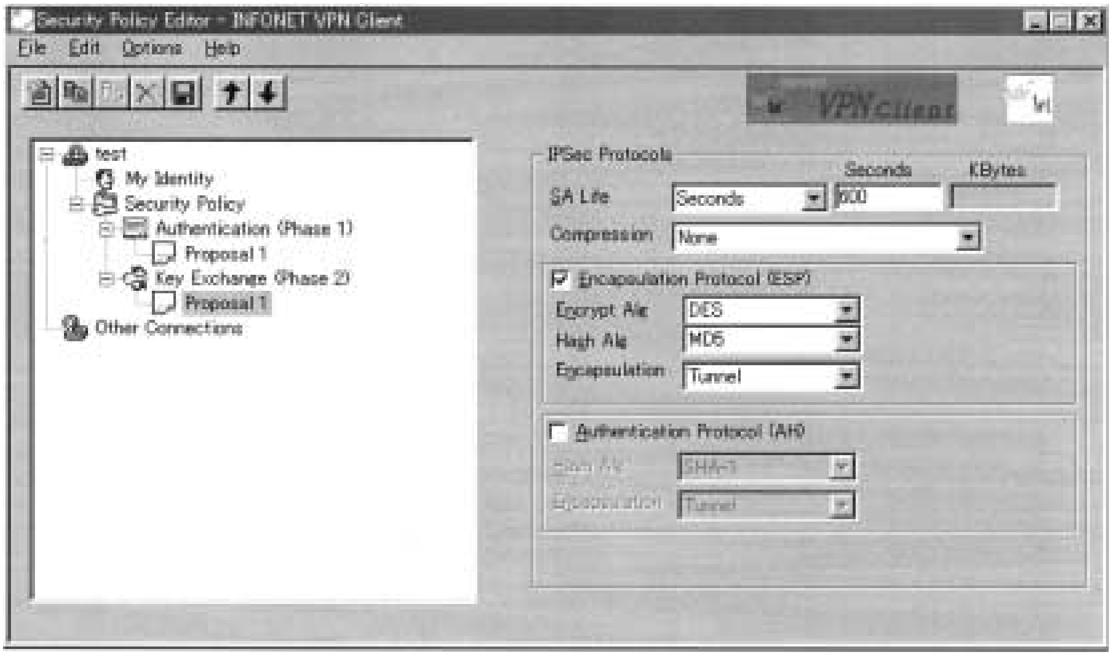
Encrypt Alg：DES※
Hash Alg　：MD５※
SA Life　　：1000 seconds※

Key Group

Diffie-Hellman Group１※

※：この設定は、IPsec トンネルを確立する相手と同じでなくてはいけません。

7. 左側のアイコン「Key Exchange（Phase２)」の「＋」をクリックしてメニューを開きます。
「Proposal１」をクリックして選択し、以下の図のように設定します。



IPSec Protocols
SA Life　　　：600 seconds※

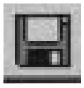
Encapsulation Protocol（ESP）－＞ チェックあり
Encrypt Alg　：DES※
Hash Alg　　：MD５※
Encapsulation：Tunnel

Authentication Protocol（AH）－＞ チェックなし

※：この設定は、IPsec トンネルを確立する相手と同じでなくてはいけません。

8. VPN として通過させたいネットワークあるいは IP アドレス毎に一つのコネクションを作成します。

9. 新しいコネクション毎について、「test」と同様に 4～7 の設定を行います。設定項目および入力値については、「test」と同じです。

10. すべての設定が完了したら、ツールバーの  をクリックし、設定を保存します。

ステップ 7
セキュリティポリシーの配布

INFONET VPN Client では、VPN の管理者が他のユーザのセキュリティポリシーを設定して、その内容を、各ユーザに配布することができます。この機能により、各ユーザは煩雑なセキュリティポリシーの設定を行うことなく VPN 通信を行うことができます。

1. VPN の管理者は、他のユーザのセキュリティポリシーを設定します。

2. Security Policy Editor 画面のファイルメニューで、「Export Security Policy」を選択します。セキュリティ・ポリシーを保護（ロック）するかどうかを尋ねるダイアログ・ボックスが表示されます。

No をクリックした場合は、セキュリティ・ポリシーを Security Policy Editor にインポートして編集することができます。

Yes をクリックした場合、セキュリティ・ポリシーはロックされて編集不可になり、エンドユーザはセキュリティ・ポリシーを変更できません。

3. 名前をつけて保存画面で、保存します。

4. 保存したファイルを、各ユーザに渡します。このファイルは、フロッピーディスクで手渡しする等の方法で渡してください。このファイルが盗まれると、セキュリティは確保できません。

5. 他のユーザの端末で、Security Policy Editor を起動します。

6. Security Policy Editor 画面のファイルメニューで、「Import Security Policy」を選択します。「開く」画面で、VPN の管理者から渡されたセキュリティポリシーのファイルを選択し、インポートします。

以上で、セキュリティポリシーの配布は完了です。

ステップ８

補　足（重要）

１つの端末を、

- **社内 LAN に接続してサーバにアクセスする**
- **社外からインターネットを介して社内のサーバにアクセスする**

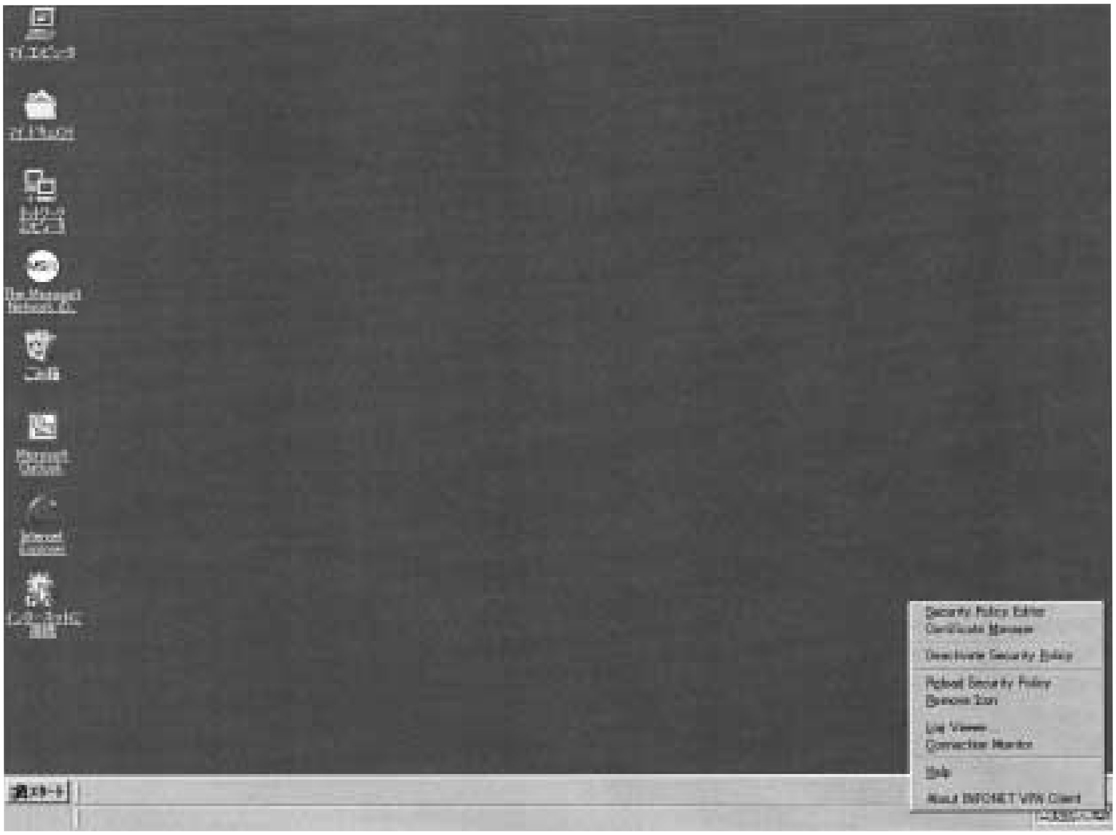
のように兼用する場合には、使用時に注意が必要になります。
社内 LAN を使用する場合には、VPN による暗号化を行う必要がなく、社外からアクセスする場合には、暗号化を行う必要があるためです。

１. 社内で利用される端末を VPN 端末として兼用する場合は、以下のオペレーションを行ってください。

⑴**タスクバーのアイコンを右クリックすると、メニューが表示されます。**

⑵**社内 LAN に接続して利用される場合には、［Deactivate Security Policy］を選択し、VPN を OFF（Deactivate Activate）状態にしてください。**
※［Activate Security Policy］　と表示される時は、すでに VPN は OFF 状態です。

⑶**社外に出て、外部からインターネットを経由してして利用される場合には、［Activate Security Policy］を選択し、VPN 機能を ON（Activate）状態にしてください。**
※［Deactivate Security Policy］　と表示される時は、すでに VPN は ON 状態です。



参考　サーバ側の設定例

1. pre-shared キーを使用する場合

・MUCHO－EV の場合

```
conf# vpn on←VPN 機能を使用する
conf# vpnpolicy add id=1 sec=600 encr=des auth=hmac－md5
          ←Phase2の認証/暗号化方式，Lifetime の指定
             【INFONET VPN Client での設定→P24】
conf# vpnpeer add name=RemoteClientl key=a, thisispresharedkey nat=off
          ←トンネルの相手の情報を設定
             【INFONET VPN Client での設定→P20、21】
conf# vpnselector add id=1 dst=192.168.100.1,255.255.255.255
src=192.168.0.0,255.255.0.0 type=ipsec peername=RemoteClientl policy=1
          ←VPN 対象パケットを指定します.
conf# vpnparam pllifesec=1000
             【INFONET VPN Client での設定→P23】
```

・INFONET－VP100, MUCHO－EV/PK の場合

```
conf# vpn on←VPN 機能を使用する
conf# vpnikepolicy add id=1 encr=des method=prekey group=1
          ←Phase1の認証方式，pre-shared の指定
             【INFONET VPN Client での設定→P23】
conf# vpnpolicy add id=1 sec=600 encr=des auth=hmac－md5
          ←Phase2の認証/暗号化方式，Lifetime の指定
             【INFONET VPN Client での設定→P24】
conf# vpnpeer add name=RemoteClientl key=a, thisispresharedkey nat=off ikepolicy=1
          ←トンネルの情報を設定
             【INFONET VPN Client での設定→P20、21】
conf# vpnselector add id=1 dst=192.168.100.1,255.255.255.255
src=192.168.0.0,255.255.0.0 type=ipsec peername=RemoteClientl policy=1
          ←VPN 対象パケットを指定
conf# vpnparam pllifesec=1000
             【INFONET VPN Client での設定→P23】
```

2．X.509を使用する場合

```
conf# vpn on←VPN 機能を使用する
conf# vpngenkey←まず、鍵ペアの生成
conf# vpncertparam crl=notuse domainname=testname.co.jp
          ←証明書に入れる、ドメイン名、IP アドレスの設定（CRL 使用しない場合）
conf# exit
configuration modified. save OK ? (y/n) ： y

Please reset# vpncertreq CN=TestRouter O=furukawa C=jp
          ←証明書リクエストの生成

             【証明書の取得】

conf# vpncert add←証明書の保存
conf# vpncert add root←CA の証明書の保存
conf# vpnikepolicy add id=1 encr=des method=rsasig group=1
          ←Phase1の認証方式，rsasig (X.509)の指定
             【INFONET VPN Client での設定→P30】
conf# vpnpolicy id=1 sec=600 encr=des auth=hmac－md5
          ←Phase2の認証/暗号化方式，Lifetime の指定
             【INFONET VPN Client での設定→P31】
conf# vpnpeer add name=RemoteClientl nat=off ikepolicy=1
          ←トンネルの情報を設定
             【INFONET VPN Client での設定→P28】
conf# vpnselector add id=1 dst=192.168.100.1,255.255.255.255
src=192.168.0.0,255.255.0.0 type=ipsec peername=RemoteClientl policy=1
          ←VPN 対象パケットを指定
conf# vpnparam pllifesec=1000
             【INFONET VPN Client での設定→P30】
```

詳しいコマンドの説明は，各センター装置の取扱説明書・コマンドリファレンスをご参照ください。

メ　　モ

メ　　　モ

メ　　モ

SafeNet™

古河電工

このマニュアルは再生紙を使用しております。

130-M0563-AH01